(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－266475

(43)公開日　平成９年(1997)10月７日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ　12/22		9466－5K	Ｈ０４Ｌ	11/26	
Ｇ０６Ｆ　15/00	３３０		Ｇ０６Ｆ	15/00	３３０Ａ
Ｇ０９Ｃ　1/00	６４０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６４０Ｚ
	６６０	7259－5Ｊ			６６０Ｅ
Ｈ０４Ｌ　9/32			Ｈ０４Ｌ	9/00	６７１

審査請求　未請求　請求項の数４　ＯＬ　（全５頁）

(21)出願番号　特願平8－73601

(22)出願日　平成８年(1996)３月28日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　澤田　素直
神奈川県川崎市幸区鹿島田890番地の12株式会社日立製作所情報・通信開発本部内

(72)発明者　菅原　征勝
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(72)発明者　西川　慈海
神奈川県横浜市戸塚区戸塚町5030番地株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　小川　勝男

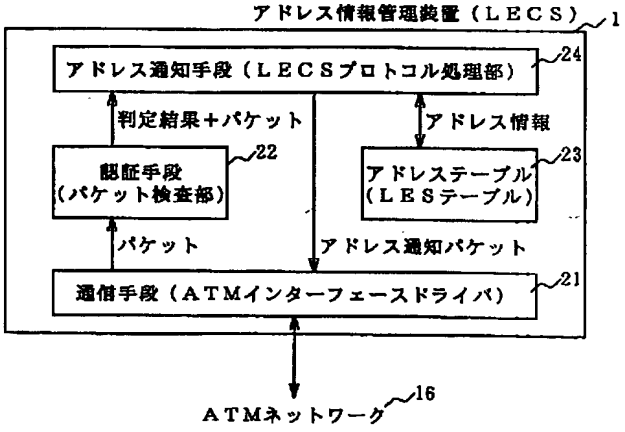
(54)【発明の名称】　アドレス情報管理装置およびネットワークシステム

(57)【要約】

【課題】不正な要求元に対してアドレス情報の通知を拒否したことを知られることなく正しいアドレス情報を渡すことを防ぎ、不正なアクセスの記録を取ることを可能にするアドレス情報管理方法を提供する。

【解決手段】アドレス情報管理装置１は通信手段２１、認証手段２２、アドレステーブル２３、アドレス通知手段２４より構成される。

図２



1

【特許請求の範囲】

【請求項１】ネットワークに接続された一または複数のネットワーク端末装置のアドレスを保持するアドレステーブルと、前記ネットワークを介して通信する通信手段と、前記通信手段により受信した要求メッセージに応じて前記アドレステーブルに登録されたアドレスから適当なものを選択し前記通信手段を介して通知するアドレス通知手段と、前記通信手段により受信した要求メッセージの内容及び要求元アドレスから要求元が正規の使用者であるか不正な使用者であるかを識別する認証手段とを含み、前記ネットワークを介して任意のネットワーク端末のアドレスの通知を要求されたとき、要求元が前記認証手段で不正な使用者であると識別された場合、前記アドレス通知手段が通知するアドレスが本来通知すべきアドレスとは異なるあらかじめ指定したアドレスであることを特徴とするアドレス情報管理装置。

【請求項２】前記認証手段により要求元が不正な使用者であると識別した場合に前記アドレス通知手段が通知するアドレスが、不正な使用者がアドレスを要求したネットワーク端末の動作を模倣する機能を有するネットワーク端末のアドレスである請求項１に記載のアドレス情報管理装置。

【請求項３】前記認証手段により要求元が不正な使用者であると識別した場合に前記アドレス通知手段が通知するアドレスが、通信内容や端末に対する操作の記録をとるトレース手段と前記トレース手段により記録された内容を保持する記憶手段とを有するネットワーク端末のアドレスである請求項１または請求項２に記載のアドレス情報管理装置。

【請求項４】請求項３に記載のアドレス情報管理装置と、前記トレース手段と前記記憶手段を有するネットワーク端末を用いて不正な要求元からの通信を記録するネットワークシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はアドレス情報管理装置およびネットワークシステムに関する。

【０００２】

【従来の技術】ネットワークを介してネットワーク端末間で通信を行う場合、通信先のアドレスが必要になる。通信先のアドレスを取得する方法として、Domain Name System（ＤＮＳ）プロトコルやＡＴＭ Forum のＬＡＮ Emulation などでは、ネットワーク端末のアドレス情報のテーブルを持っているサーバに問い合わせを行う方式が用いられている。

【０００３】この方式では、不正な使用者にアドレス情報が知られることを防ぐために、要求元のアドレスや要求メッセージの内容を検査し、アドレス情報を通知すべきか否かを決定する方法が一般的に用いられている（例えば「インターネット接続でのファイアウォールセキュリティ管理技術」ソフトバンク発行の３３ページ）。

2

【０００４】

【発明が解決しようとする課題】従来の方法では、不正な要求元に対してアドレス情報を通知することは防げるが、アドレス情報の取得が失敗したことが不正な使用者にもわかってしまう。このため不正な使用者は要求メッセージ内のパラメータを次々に変えて何度も要求を繰り返すことができ、この繰り返しにより正しいパラメータが発見されれば、不正な使用者がアドレス情報を取得することが可能になってしまう。また、正しいパラメータが発見できない場合でも、不正な使用者による要求を処理するための負荷がアドレス情報管理装置にかかり、正規の使用者の処理が遅くなるなどの問題が生じる恐れがある。さらに、不正な要求を拒否するだけでは、その要求元がどこであるかその意図は何であるかといったことがわからなくなってしまうという問題がある。

【０００５】本発明の目的は、正常なアドレスに見せかけた別のアドレスを不正な使用者に通知することで、不正な使用者が正しいアドレスを取得することを防ぎ、かつアドレス情報管理装置の処理を軽減し、さらに不正な使用者からのアクセスを記録する方法およびそれを用いたアドレス情報管理方式を提供することにある。

【０００６】

【課題を解決するための手段】上記の目的を達成するため、本発明のアドレス情報管理装置は、アドレステーブル、通信手段、認証手段を含む構成とする。通信手段により受信したメッセージは認証手段により検査され、正規の使用者である場合はアドレステーブル中の必要な情報を通知し、不正な使用者に対してはあらかじめ指定されたアドレスを通知する。

【０００７】本発明によれば、認証手段により不正な要求元からのメッセージと判断された要求に対しては、あらかじめ指定されたアドレスを通知するため、要求元ではアドレス取得が成功したか失敗したかを判断できない。不正な要求元に通知するアドレスとして、重要な情報を持たず誰がアクセスしても差し支えない端末のアドレスを用意しておけば、不正な使用者に重要な情報を渡すことを防げ、かつ正しいアドレスの取得が失敗したことを知られることもない。

【０００８】また本発明で、不正な要求元に通知するアドレスを通信内容の記録を取る機能を持つ端末のアドレスとすることにより、不正なアクセスの記録を残し要求元の特定作業などを支援することが可能になる。

【０００９】

【発明の実施の形態】次に、本発明の各実施例について説明する。図１は本発明によるアドレス情報管理方式の第１実施例のネットワークシステムである。この図はＡＴＭ（Asynchronous Transfer Mode)ネットワークにより相互に接続された端末間で、ＡＴＭ Forum標準のＬＡＮ Emulation を用いて通信を行うネットワークシ

ステムを示している。

【0010】図1のLECS（LAN Emulation Configuration Server）は本発明によるアドレス情報管理装置1の一つの実施例である。図2に内部のソフトウェア構造を示す。図2に於けるATMインターフェースドライバはATMネットワークで通信を行う通信手段21であり、パケット検査部はパケットの内容に基づいて要求元を識別する認証手段22、LESテーブルはLES（LAN EmulationServer）2のアドレスを登録してあるアドレステーブル23、LECSプロトコル処理部は要求元に対してLES2のアドレスを回答するアドレス通知手段24である。

【0011】ATMインターフェースドライバ21はLES2のアドレスを要求するパケットを受信すると、パケット検査部22へとそのパケットを渡す。パケット検査部22ではパケットのSOURCE－LAN－DESTINATIONフィールド309およびSOURCE－ATM－ADDRESSフィールド311（図3参照）に格納されている要求元のアドレスと、ELAN－NAMEフィールド3 1-7の内容を検査し、あらかじめ設定されている値の範囲に合致した場合に有効、そうでない場合に不正な要求であると判定し、判定結果をパケットとともにLECSプロトコル処理部24へ通知する。LECSプロトコル処理部24では判定結果が有効だった場合にはLESテーブル23を検索し、LES2のアドレスを含んだアドレス通知パケットを作ってATMインターフェースドライバ21を介して要求元へと通知する。判定結果が不正だった場合、侵入対策用端末11（図1）のアドレスを含んだアドレス通知パケットをATMインターフェースドライバ21を介して要求元へ通知する。

【0012】図1のネットワークシステムに於いて、不正な要求元12がLECS1に対してLES2のアドレスを要求した場合のシーケンスを図4にそって説明する。まず、不正な要求元12がLECS1に対してLES2のアドレスを要求する（401）。LECS1は要求パケットの発信元アドレス等の検査から、この要求が不正な使用者によるものであると判断し（402）、LES2ではなく侵入対策用端末11のアドレスを通知する（403）。不正な要求元12は通知されたアドレス（侵入対策用端末11のアドレス）に対して接続を試み（404）許可される（405）。

【0013】この例における侵入対策用端末11は、LES2と同等の機能を有し、LES2と同じように動作するが、正規の使用者からのアクセスは行われないように設定してある。また、侵入対策用端末11には、重要な情報、例えば、他のLEC（LAN Emulation Client）13、14、15のアドレスなど、は入れないでおく。不正な要求元12では接続相手がLES2だと考え、情報の要求を行う（406）が、侵入対策用端末1

1には該当する情報がないので、情報無しという回答（407）しか得られない。

【0014】以上のように、本実施例のネットワークシステムでは不正な要求に対してLECS1が侵入対策用端末11のアドレスを通知するため、要求が認められたか拒否されたかが不正な要求元には判断がつかない。また、不正なアクセスの対象となる侵入対策用端末11には重要な情報がないため、不正な使用者が何らかの重要な情報を入手することを防げる。

【0015】図5に本発明によるアドレス情報管理方式の第2実施例であるネットワークシステムを示す。このネットワークシステムでは、各端末がDNSネームサーバ51に問い合わせを行うことで通信先端末のアドレスを得て通信を行う。

【0016】図5のDNSネームサーバ51は本発明によるアドレス情報管理装置の一つの実施例である。図6にDNSネームサーバ51のソフトウェア構造を示す。通信プロトコル処理部61はネットワークにパケットを送受信する通信手段、ソースアドレス検査部62はパケットの送信元アドレスを検査して、正規の要求元であるか不正な要求元であるかを判断する認証手段、DNSプロトコル処理部63は要求パケットが正規の要求元である場合にアドレスを通知するアドレス通知手段であり、ホストテーブル64はネットワークシステムに接続されている各端末54、55、56のアドレスが登録されているアドレステーブルである。

【0017】DNSプロトコル処理部63は正規の使用者54、55、56に対してはホストテーブル64を検索して結果を通知し、不正な要求元52に対しては通信記録用端末53のアドレスを通知する。不正な要求元52は通知されたアドレス（通信記録用端末53のアドレス）に対して通信を行う。通信記録用端末53は受信したパケットの内容を記録する機能を持つ。通信記録用端末53は不正な要求元52からの通信に対して通信プロトコルの規定に沿って応答を返すが、重要なデータを内部に持たないため、不正な使用者がデータを入手することはない。パケット内容の記録は、要求元のアドレス割り出しや使用者の目的の解析などに有効である。

【0018】以上のように本実施例では不正な要求元52に通知するアドレスを通信記録機能を持つ端末のアドレスにすることで、不正な要求元52との通信記録を残し、要求元のアドレス割り出しなどの解析が行えるという特徴がある。

【0019】

【発明の効果】本発明のアドレス情報管理装置およびそれを用いたネットワークシステムによれば、不正な要求元に対してあらかじめ用意したアドレスを通知することで、情報の要求を拒否したことを知られること無しに重要な情報を渡さないアドレス情報管理ができる。また、通知するアドレスを通信記録機能を持つ端末のアドレス

5

とすることで、不正な要求元からの通信内容を記録し、要求元のアドレスやアクセスの意図を解析するためのデータを残すことが可能になる。

【図面の簡単な説明】

【図１】本発明によるネットワークシステムの第１実施例の説明図。

【図２】本発明によるアドレス情報管理装置のソフトウェアの説明図。

【図３】アドレス要求パケットのフォーマットの説明図。

【図４】不正なアドレス要求に対する動作シーケンスの説明図。

6

【図５】本発明によるネットワークシステムの第２実施例の説明図。

【図６】ＤＮＳネームサーバのブロック図。

【符号の説明】

１…アドレス情報管理装置、

１１…侵入対策用端末、

１２…不正な要求元、

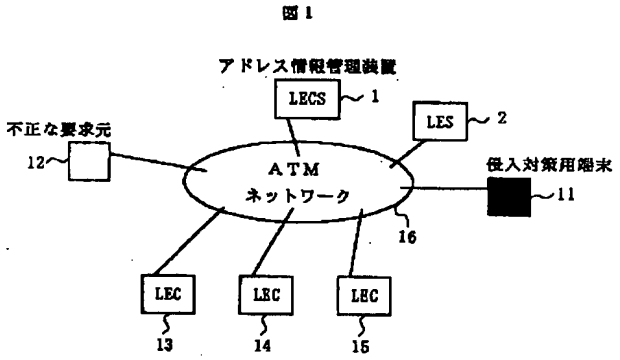
２１…通信手段、

２２…認証手段、

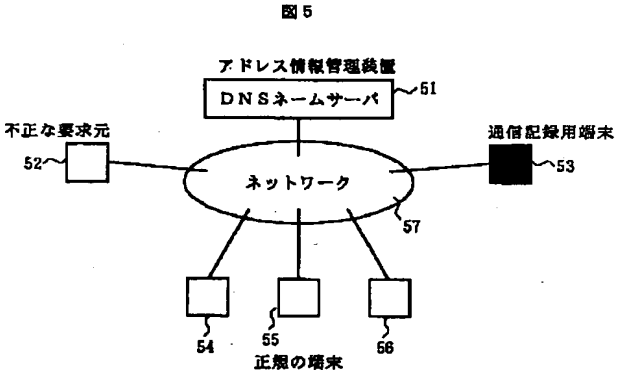
２３…アドレステーブル、

２４…アドレス通知手段。

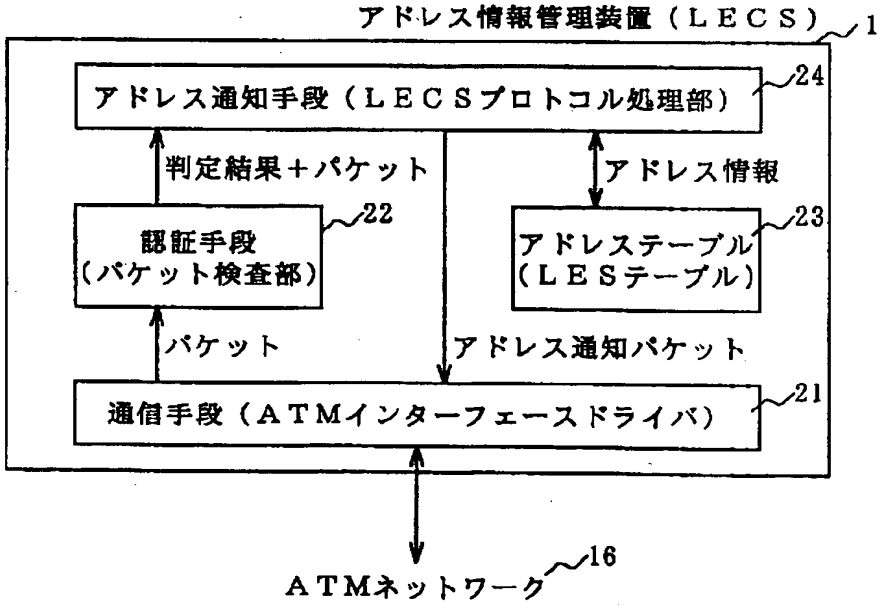
【図１】



【図５】

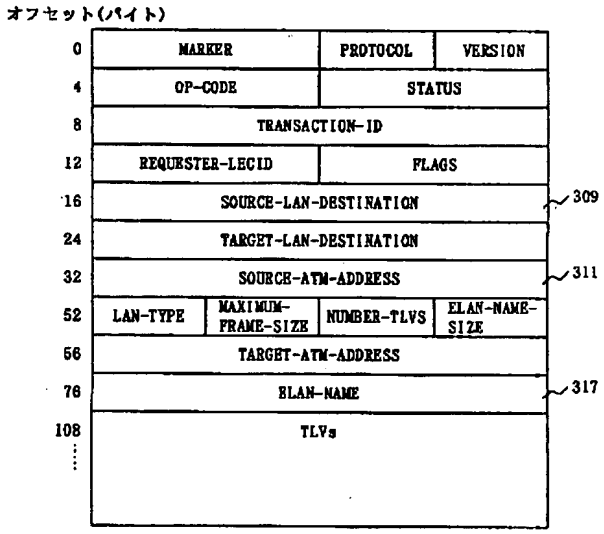


【図２】



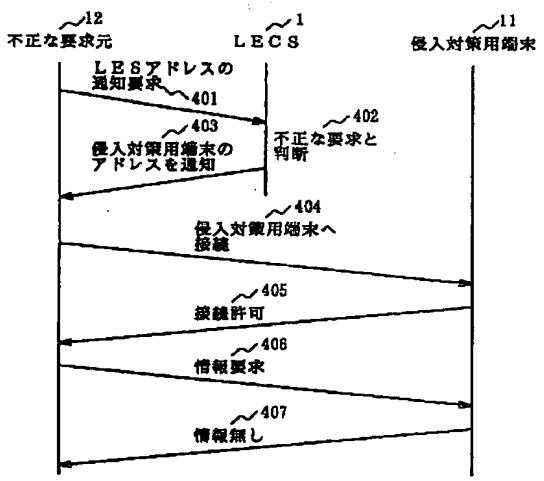
【図３】

図３



【図４】

図４



【図６】

図６